

BURSOR & FISHER, P.A.
L. Timothy Fisher (State Bar No. 191626)
Brittany S. Scott (State Bar No. 327132)
1990 North California Blvd., Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-mail: ltfisher@bursor.com
bscott@bursor.com

Attorneys for Plaintiff

**UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA**

BRANDON GRAY, individually and on
behalf of all others similarly situated,

Plaintiff,

v.

LUXOTTICA OF AMERICA INC. d/b/a
LENSCRAFTERS,

Defendant.

Case No. 8:24-cv-160

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

1 Plaintiff Brandon Gray (“Plaintiff”) brings this class action complaint on
2 behalf of himself and all others similarly situated (the “Class Members”) against
3 Defendant Luxottica of America Inc. (“Defendant” or “LensCrafters”). Plaintiff
4 brings this action based on personal knowledge of the facts pertaining to himself, and
5 on information and belief as to all other matters, by and through the investigation of
6 undersigned counsel.

7 **NATURE OF THE ACTION**

8 1. This is a class action brought on behalf of all California residents who
9 have accessed and used www.lenscrafters.com (the “Website”), a website Defendant
10 owns and operates.

11 2. Defendant aided, employed, agreed, and conspired with Facebook¹ to
12 intercept communications sent and received by Plaintiff and Class Members,
13 including communications containing protected medical information. Plaintiff
14 brings this action for legal and equitable remedies resulting from these illegal
15 actions.

16 **JURISTITION AND VENUE**

17 3. The Court has subject matter jurisdiction pursuant to 28
18 U.S.C. § 1332(d)(2)(A), as amended by the Class Action Fairness Act of 2005
19 “CAFA”), because this case is a class action where the aggregate claims of all
20 members of the proposed class are in excess of \$5,000,000.00, exclusive of interest
21 and costs, there are over 100 members of the putative class, and Plaintiff, as well as
22 most members of the proposed class, is a citizen of a state different from Defendant.

23 4. This Court has personal jurisdiction over the parties because Plaintiff
24 resides in California, is a citizen of California, and submits to the jurisdiction of the
25 Court. Further, Defendant has, at all times relevant hereto, systematically and

26
27 ¹ In October 2021, Facebook, Inc. changed its name to Meta Platforms, Inc. Unless
28 otherwise indicated, Facebook, Inc. and Meta Platforms, Inc. are referenced
collectively as “Facebook.”

continually conducted business in California, including within this District, and/or intentionally availed itself of the benefits and privileges of the California consumer market through the promotion, marketing, and sale of its products and/or services to residents within this District and throughout California. Additionally, Plaintiff, while in California, scheduled an eye exam at one of Defendant's California locations using Defendant's Website.

PARTIES

Defendant

5. Defendant, Luxottica of America, Inc., d/b/a LensCrafters, is incorporated in Ohio with its principal place of business in Mason, Ohio. Defendant owns and operates the website www.lenscrafters.com. Defendant provides a range of prescription eyeglasses and contact lenses as well as routine eye exams for consumers to maintain their eye health².

Plaintiff

6. Plaintiff Brandon Gray is an adult citizen of California domiciled in La Habra, California.

7. Plaintiff Gray has used LensCrafter's Website for numerous years. Plaintiff's use of the Website consisted, and consists, of scheduling eye exams with Defendant to obtain new eye prescriptions.

8. During the time Plaintiff Gray used LensCrafter's Website, he maintained a social media account with Facebook. Plaintiff Gray used the same device to access the Website and his Facebook account. Subsequently, as a result of Defendant's disclosures, he received advertisements on Facebook and Instagram relating to vision care.

² See, LENS CRAFTERS, <https://www.lenscrafters.com/lc-us/about-lenscrafters>.

1 9. Since December 2007, Plaintiff Gray has had an active Facebook
2 account. Plaintiff routinely accessed his Facebook account using his smartphone and
3 computer.

4 10. Pursuant to the systematic process described herein, Defendant assisted
5 Facebook with intercepting Plaintiff Gray's communications, including those that
6 contained personally identifiable information, protected health information, and
7 related confidential information. Defendant assisted these interceptions without
8 Plaintiff Gray's knowledge, consent, or express written authorization.

9 11. By failing to receive the requisite consent, Defendant breached its duties
10 of confidentiality and unlawfully disclosed Plaintiff Gray's personally identifiable
11 information and protected health information.

12 **FACTUAL ALLEGATIONS**

13 **A. Background of the California Information Privacy Act ("CIPA")**

14 12. The CIPA, Cal. Penal Code § 630, *et seq.*, prohibits aiding or permitting
15 another person to willfully—and without the consent of all parties to a
16 communication—read or learn the contents or meaning of any message, report, or
17 communication while the same is in transit or passing over any wire, line, or cable,
18 or is being sent from or received at any place within California.

19 13. To establish liability under Cal. Penal Code § 631(a), a plaintiff need
20 only establish that the defendant, "by means of any machine, instrument,
21 contrivance, or in any other manner," does any of the following:

22
23 Intentionally taps, or makes any unauthorized connection, whether physically,
24 electrically, acoustically, inductively or otherwise, with any telegraph or
25 telephone wire, line, cable, or instrument, including the wire, line, cable, or
instrument of any internal telephonic communication system,

26 Or

27 Willfully and without the consent of all parties to the communication, or in any
28 unauthorized manner, reads or attempts to read or learn the contents or meaning

1 of any message, report, or communication while the same is in transit or passing
2 over any wire, line or cable or is being sent from or received at any place within
3 this state,

4 Or

5 Aids, agrees with, employs, or conspires with any person or persons to
6 unlawfully do, or permit, or cause to be done any of the acts or things mentioned
7 above in this section.

8 14. Section 631(a)'s applicability is not limited to phone lines, but also
9 applies to "new technologies" such as computers, the internet, and email. *See*
10 *Matera v. Google Inc.*, 2016 WL 8200619, at *21 (N.D. Cal. Aug. 12, 2016) (CIPA
11 applies to "new technologies" and must be construed broadly to effectuate its
12 remedial purpose of protecting privacy); *Bradley v. Google, Inc.*, 2006 WL 3798134,
13 at *5-6 (N.D. Cal. Dec. 22, 2006) (CIPA governs "electronic communications"); *In*
14 *re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589 (9th Cir. 2020)
15 (reversing dismissal of CIPA and common law privacy claims based on Facebook's
16 collection of consumers' internet browsing history).

17 15. Under Cal. Penal Code § 637.2, Plaintiff and Class Members may seek
18 injunctive relief and statutory damages of \$5,000 per violation.

19 **B. Background of the California Confidentiality of**
20 **Medical Information Act**

21 16. Pursuant to the California Confidentiality of Medical Information Act
22 ("CMIA"), a "provider of health care ... shall not disclose medical information
23 regarding a patient of the provider of health care ... without first obtaining an
24 authorization, except as provided in subdivision (b) or (c)." Cal Civ. Code §
25 56.10(a).³ "An authorization for the release of medical information ... shall be valid
26 if it:

27 ³ Subdivisions (b) and (c) are not relevant to this case but permit the disclosure of
28 medical information in situations where a government investigation or lawsuit is

1 (a) Is handwritten by the person who signs it or is in a typeface no smaller
2 than 14-point type.

3 (b) Is clearly separate from any other language present on the same page
4 and is executed by a signature which serves no other purpose than to
5 execute the authorization.

6 (c) Is signed and dated ...

7 (d) States the specific uses and limitations on the types of medical
8 information to be disclosed.

9 (e) States the name or functions of the provider of health care, health care
10 service plan, pharmaceutical company, or contractor that may disclose
11 the medical information.

12 (f) States the name or functions of the persons or entities authorized to
13 receive the medical information.

14 (g) States the specific uses and limitations on the use of the medical
15 information by the persons or entities authorized to receive the medical
16 information.

17 (h) States a specific date after which the provider of health care, health
18 care service plan, pharmaceutical company, or contractor is no longer
19 authorized to disclose the medical information.

20 (i) Advises the person signing the authorization of the right to receive a copy of
21 the authorization.”

22 Cal. Civ. Code § 56.11.

23 17. Moreover, a health care provider that maintains information for
24 purposes covered by the CMIA is liable for negligent disclosures that arise as the
25 result of an affirmative act—such as implementing a system that records and

26 _____
27 taking place. For example, Defendant could bypass the authorization requirement if
28 patient medical information was requested pursuant to a lawful court order or by a
party to a proceeding before a court or administrative agency pursuant to a subpoena.
See Cal. Civ. Code §§ 56.10(b)(3) and 56.10(b)(6).

discloses online patients' personally identifiable information and protected health information. Cal. Civ. Code § 56.36(c).⁴ Similarly, if a negligent release occurs and medical information concerning a patient is improperly viewed or otherwise accessed, the individual need not suffer actual damages. Cal. Civ. Code § 56.36(b).

18. "In addition to any other remedies available at law, any individual may bring an action against any person or entity who has negligently released confidential information or records concerning him or her in violation of this part, for either or both of the following: [¶] (1) ... nominal damages of one thousand dollars (\$1,000). In order to recover under this paragraph, it shall not be necessary that the plaintiff suffered or was threatened with actual damages. [¶] (2) The amount of actual damages, if any, sustained by the patient." *Sutter Health v. Superior Ct.*, 227 Cal. App. 4th 1546, 1551, 174 Cal. Rptr. 3d 653, 656 (2014) (quoting Cal. Civ. Code § 56.36(b)).

C. Defendant's Website

19. Defendant is a corporation that focuses on delivering prescription eyewear, such as eyeglasses and contact lenses, to its consumers.⁵ Defendant also provides its consumers with eye health care services, such as routine eye exams to maintain eye health care.⁶

20. Defendant's Website, www.lenscrafters.com, is accessible on mobile devices and desktop computers.

⁴ "Every provider of health care ... who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall do so in a manner that preserves the confidentiality of the information contained therein. Any provider of health care ... who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to the remedies and penalties provided under subdivisions (b) and (c) of Section 56.36." Cal. Civ. Code § 56.101, subd. (a).

⁵ See, *supra* note 2.

⁶ *Id.*

D. Facebook’s Platform and its Business Tools

21. Facebook describes itself as a “real identity platform,”⁷ meaning users are allowed only one account and must share “the name they go by in everyday life.”⁸ To that end, when creating an account, users must provide their first and last name, along with their birthday and gender.⁹

22. In 2021, Facebook generated over \$117 billion in revenue.¹⁰ With respect to the apps offered by Facebook, substantially all of Facebook’s revenue is generated by selling advertising space.¹¹

23. Facebook sells advertising space by highlighting its ability to target users.¹² Facebook can target users so effectively because it surveils user activity both on and off its site.¹³ This allows Facebook to make inferences about users beyond what they explicitly disclose, like their “interests,” “behavior,” and “connections.”¹⁴ Facebook compiles this information into a generalized dataset called “Core Audiences,” which allows advertisers to reach precise audiences based on specified targeting types.¹⁵

⁷ Sam Schechner and Jeff Horwitz, *How Many Users Does Facebook Have? The Company Struggles to Figure It Out*, WALL. ST. J. (Oct. 21, 2021).

⁸ FACEBOOK, COMMUNITY STANDARDS, PART IV INTEGRITY AND AUTHENTICITY, https://www.facebook.com/communitystandards/integrity_authenticity.

⁹ FACEBOOK, SIGN UP, <https://www.facebook.com>.

¹⁰ FACEBOOK, META ANNUAL REPORT 2021, https://s21.q4cdn.com/399680738/files/doc_financials/annual_reports/2023/2021-Annual-Report.pdf at 51.

¹¹ *Id.* at 63.

¹² FACEBOOK, WHY ADVERTISE ON FACEBOOK, INSTAGRAM AND OTHER META TECHNOLOGIES, <https://www.facebook.com/business/help/205029060038706>.

¹³ FACEBOOK, ABOUT META PIXEL, <https://www.facebook.com/business/help/742478679120153?id=1205376682832142>.

¹⁴ FACEBOOK, AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, <https://www.facebook.com/business/ads/ad-targeting>.

¹⁵ <https://www.facebook.com/business/news/Core-Audiences>.

1 24. Advertisers can also build “Custom Audiences.”¹⁶ Custom Audiences
2 enables advertisers to reach “people who have already shown interest in [their]
3 business, whether they’re loyal customers or people who have used [their] app or
4 visited [their] website.”¹⁷ With Custom Audiences, advertisers can target existing
5 customers directly, and they can also build “Lookalike Audiences,” which
6 “leverage[] information such as demographics, interests, and behavior from your
7 source audience to find new people who share similar qualities.”¹⁸ Unlike Core
8 Audiences, advertisers can build Custom Audiences and Lookalike Audiences only if
9 they first supply Facebook with the underlying data. They can do so through two
10 mechanisms: by manually uploading contact information for customers or by
11 utilizing Facebook’s “Business Tools.”¹⁹

12 25. As Facebook puts it, the Business Tools “help website owners and
13 publishers, app developers, and business partners, including advertisers and others,
14 integrate with [Facebook], understand and measure their products and services, and
15 better reach and serve people who might be interested in their products and
16 services.”²⁰ Put more succinctly, Facebook’s Business Tools are bits of code that
17 advertisers can integrate into their websites, mobile applications, and servers, thereby
18 enabling Facebook to intercept and collect user activity on those platforms.

19 26. The Business Tools are automatically configured to capture certain data,

20 ¹⁶ FACEBOOK, ABOUT CUSTOM AUDIENCES,
21 <https://www.facebook.com/business/help/744354708981227?id=2469097953376494>.

22 ¹⁷ FACEBOOK, AD TARGETING, HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR
23 BUSINESS, <https://www.facebook.com/business/ads/ad-targeting>.

24 ¹⁸ FACEBOOK, ABOUT LOOKALIKE AUDIENCES,
<https://www.facebook.com/business/help/164749007013531?id=401668390442328>.

25 ¹⁹ FACEBOOK, CREATE A CUSTOMER LIST CUSTOM AUDIENCE,
26 <https://www.facebook.com/business/help/170456843145568?id=2469097953376494>;
27 FACEBOOK, CREATE A WEBSITE CUSTOM AUDIENCE,
28 <https://www.facebook.com/business/help/1474662202748341?id=2469097953376494>.

²⁰ FACEBOOK, THE META BUSINESS TOOLS,
<https://www.facebook.com/help/331509497253087>.

1 like when a user visits a webpage, that webpage's Universal Resource Locator
2 ("URL") and metadata, or when a user downloads a mobile application or makes a
3 purchase.²¹ Facebook's Business Tools can also track other events. Facebook offers
4 a menu of "standard events" from which advertisers can choose, including what
5 content a visitor views or purchases.²² Advertisers can even create their own
6 tracking parameters by building a "custom event."²³

7 27. One such Business Tool is the Facebook Tracking Pixel (the "Facebook
8 Tracking Pixel"). Facebook offers this piece of code to advertisers, like Defendant,
9 to integrate into their website. As the name implies, the Facebook Tracking Pixel
10 "tracks the people and type of actions they take."²⁴ When a user accesses a website
11 hosting the Facebook Tracking Pixel, Facebook's software script surreptitiously
12 directs the user's browser to contemporaneously send a separate message to
13 Facebook's servers. This second secret and contemporaneous transmission contains
14 the original GET request sent to the host website, along with additional data that the
15 Facebook Tracking Pixel is configured to collect. This transmission is initiated by
16 Facebook code and concurrent with the communications with the host website. At
17 relevant times, two sets of code were thus automatically run as part of the browser's
18
19

20 ²¹ See FACEBOOK, META FOR DEVELOPERS: META PIXEL, ADVANCED,
21 <https://developers.facebook.com/docs/meta-pixel/advanced/>; see also FACEBOOK,
22 BEST PRACTICES FOR META PIXEL SETUP,
23 <https://www.facebook.com/business/help/218844828315224?id=1205376682832142>;
24 FACEBOOK, META FOR DEVELOPERS: MARKETING API - APP EVENTS API,
25 <https://developers.facebook.com/docs/marketing-api/app-event-api/>.

26 ²² FACEBOOK, SPECIFICATIONS FOR META PIXEL STANDARD EVENTS,
27 <https://www.facebook.com/business/help/402791146561655?id=1205376682832142>.

28 ²³ FACEBOOK, ABOUT STANDARD AND CUSTOM WEBSITE EVENTS,
<https://www.facebook.com/business/help/964258670337005?id=1205376682832142>;
see also FACEBOOK, META FOR DEVELOPERS: MARKETING API – APP EVENTS API,
<https://developers.facebook.com/docs/marketing-api/app-event-api/>.

²⁴ FACEBOOK, RETARGETING, <https://www.facebook.com/business/goals/retargeting>.

1 attempt to load and read Defendant’s Website—Defendant’s own code and
2 Facebook’s embedded code.

3 28. Defendant chose to include the Facebook Tracking Pixel on its Website.

4 29. Facebook’s own documentation makes clear just how much tracking of
5 private information the Facebook Tracking Pixel does. It describes the Facebook
6 Tracking Pixel as code that Facebook’s business customers can put on their website
7 to “[m]ake sure your ads are shown to the right people. *Find ... people who have*
8 *visited a specific page or taken a desired action on your website.*” (Emphasis
9 added.)²⁵

10 30. Facebook instructs such business customers that:

11 Once you’ve set up the [Facebook Tracking] Pixel, *the pixel will log when*
12 *someone takes an action on your website.* Examples of actions include adding
13 an item to their shopping cart or making a purchase. *The Pixel receives these*
14 *actions, or events,* which you can view on your [Facebook Tracking] Pixel page
15 in Events Manager. From there, you’ll be able to see the actions that your
16 customers take. *You’ll also have options to reach those customers again*
17 *through future Meta ads.*²⁶

18 31. Of course, in healthcare, it is medical specialists that users “add to their
19 shopping cart.” They make optometrist appointments rather than making purchases.

20 32. The Facebook Tracking Pixel code enables Facebook not only to help
21 Defendant with advertising to its own patients outside the Website, but also include
22 individual patients among groups targeted by *other* Facebook advertisers relating to
23 the conditions about which patients communicated on Defendant’s Website.

24 33. Facebook’s Business Help Center explains:

25 Meta *uses marketing data to show ads to people who are likely to be interested*
26 *in them.* One type of marketing data is website events, which are *actions that*

27 ²⁵ Meta, ABOUT META PIXEL,
28 <https://www.facebook.com/business/help/742478679120153?id=1205376682832142>
(last visited Dec. 26, 2023).

²⁶ *Id.* (Emphasis added.)

1 *people take on your website.*²⁷

2
3 34. In other words, Facebook sells advertising space by highlighting its
4 ability to target users.²⁸ Facebook can target users so effectively because it surveils
5 user activity both on and off its site.²⁹ This allows Facebook to make inferences
6 about users beyond what they explicitly disclose, like their “interests,” “behavior,”
7 and connections.³⁰

8 35. An example illustrates how the Facebook Tracking Pixel works. Take
9 an individual who, at relevant times, navigated to Defendant’s Website and clicked
10 on a link to schedule an eye exam. When that link was clicked, the individual’s
11 browser sent a GET request to Defendant’s server requesting that server to load the
12 particular webpage. As a result of Defendant’s use of the Facebook Tracking Pixel,
13 Facebook’s embedded code, written in JavaScript, sent secret instructions back to the
14 individual’s browser, without alerting the individual that this was happening.
15 Facebook caused the browser to secretly duplicate the communication with
16 Defendant, transmitting it to Facebook’s servers, alongside additional information
17 that transcribed the communication’s content and the individual’s identity.

18 36. After collecting and intercepting the information described in the
19 preceding paragraph, Facebook processed it, analyzed it, and assimilated it into
20 datasets like Core Audiences and Custom Audiences.

21
22 ²⁷ Meta, ABOUT STANDARD AND CUSTOM WEBSITE EVENTS,
23 <https://www.facebook.com/business/help/964258670337005?id=1205376682832142>
(emphasis added).

24 ²⁸ Meta, WHY ADVERTISE ON FACEBOOK, INSTAGRAM AND OTHER META
25 TECHNOLOGIES, <https://www.facebook.com/business/help/205029060038706> (last
visited Dec. 26, 2023).

26 ²⁹ Meta, ABOUT META PIXEL,
<https://www.facebook.com/business/help/742478679120153?id=1205376682832142>.

27 ³⁰ Meta, AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR
28 BUSINESS, <https://www.facebook.com/business/ads/ad-targeting>.

E. How Defendant Disclosed Plaintiff's and Class Members' Protected Health Information and Assisted With Intercepting Communications

37. Through the Facebook Tracking Pixel, Defendant shared its patients' identities and online activity, including information related to patients' seeking eye health care like routine eye exams.

38. For example, when a patient entered Defendant's Website and began the process of booking an eye exam, Defendant transmitted the fact that the patient was booking an eye exam to Facebook through the Facebook Tracking Pixel by sharing "PageView" events detailing information about which page on Defendant's website the patient was viewing. When booking an eye exam, the PageView event information shared with Facebook includes the terms "eye-exam" and "reschedule." See Figure 1 and 2.

Figure 1

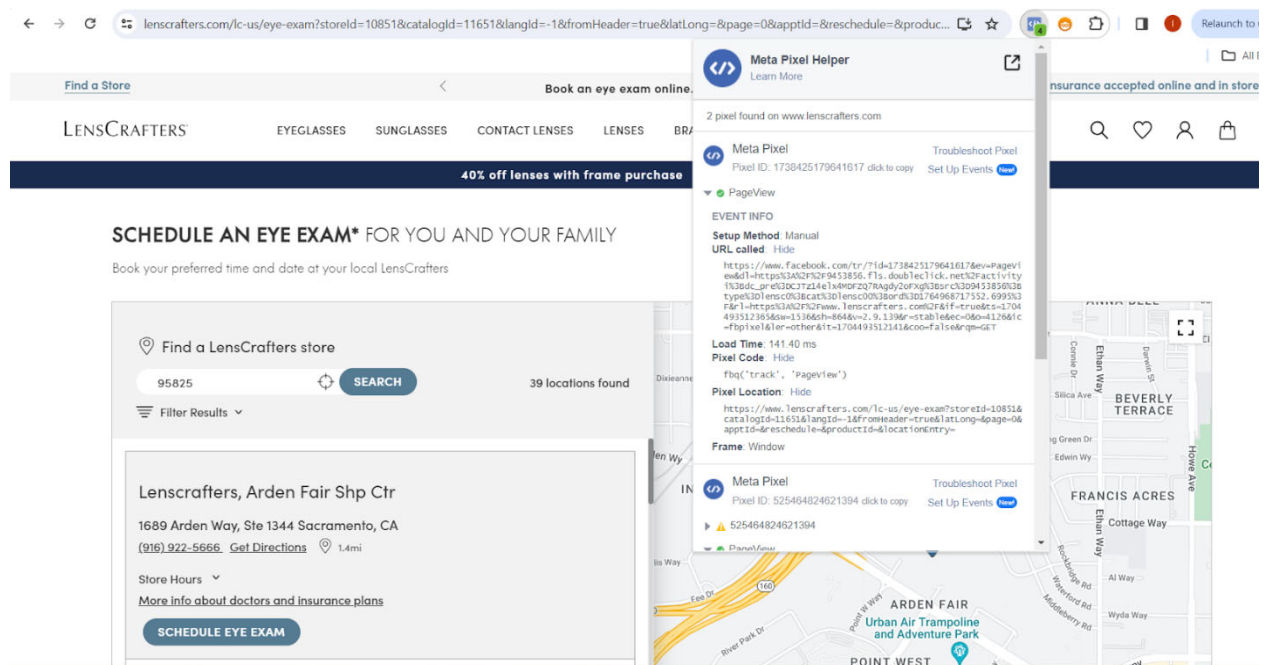
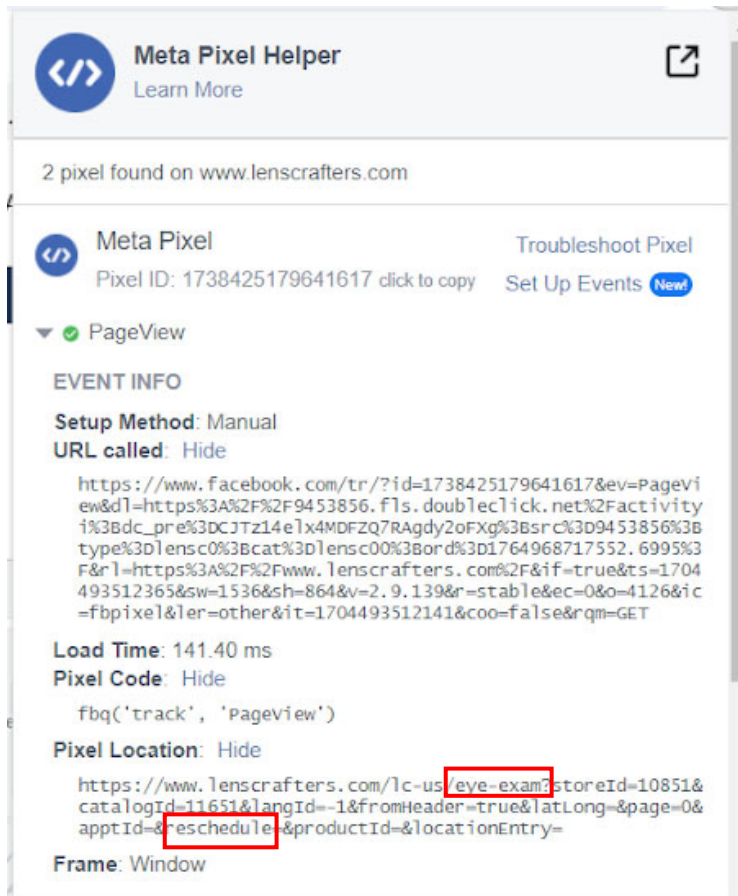


Figure 2



39. Each time Defendant sent this activity data, it also disclosed a patient's personally identifiable information, including their Facebook ID ("FID"). An FID is a unique and persistent identifier that Facebook assigns to each user. With it, any ordinary person can look up the user's Facebook profile and name. Notably, while Facebook can easily identify any individual on its Facebook platform with only their unique FID, so too can any ordinary person who comes into possession of an FID. Facebook admits as much on its website. Indeed, ordinary persons who come into possession of the FID can connect to any Facebook profile.

40. A user who accessed Defendant's Website while logged into Facebook transmitted what is known as a "c_user cookie" to Facebook, which contained that user's unencrypted Facebook ID.

1 41. When a visitor's browser had recently logged out of an account,
2 Facebook compelled the visitor's browser to send a smaller set of cookies.

3 42. One such cookie was the "fr cookie" which contained, at least, an
4 encrypted Facebook ID and browser identifier.³¹ Facebook, at a minimum, used the
5 fr cookie to identify users.³²

6 43. If a visitor had never created an account, an even smaller set of cookies
7 was transmitted.

8 44. At each stage, Defendant also utilized the "_fbp cookie," which attached
9 to a browser as a first-party cookie, and which Facebook used to identify a browser
10 and a user.³³

11 45. The c_user cookie expires after 90 days if the user checked the "keep
12 me logged in" checkbox on the website.³⁴ Otherwise, the c_user cookie is cleared
13 when the browser exits.³⁵

14 46. The fr cookie expires after 90 days unless the visitor's browser logs
15 back into Facebook.³⁶ If that happens, the time resets, and another 90 days begins to
16 accrue.³⁷

17 47. The _fbp cookie expires after 90 days unless the visitor's browser
18 accesses the same website.³⁸ If that happens, the time resets, and another 90 days

19 _____
20 ³¹ DATA PROTECTION COMMISSIONER, FACEBOOK IRELAND LTD, REPORT OF RE-
AUDIT (Sept. 21, 2012), http://www.europe-v-facebook.org/ODPC_Review.pdf.

21 ³² FACEBOOK, PRIVACY CENTER – COOKIES POLICY,
22 <https://www.facebook.com/privacy/policies/cookies/?subpage=subpage-1.3>.

23 ³³ *Id.*

24 ³⁴ Seralthan, FACEBOOK COOKIES ANALYSIS (Mar. 14, 2019),
<https://techexpertise.medium.com/facebook-cookies-analysis-e1cf6ffbfd8a>.

25 ³⁵ *Id.*

26 ³⁶ *See id.*

27 ³⁷ Confirmable through developer tools.

28 ³⁸ FACEBOOK, PRIVACY CENTER – COOKIES POLICY,
<https://www.facebook.com/privacy/policies/cookies/?subpage=subpage-1.3>.

1 begins to accrue.³⁹

2 48. The Facebook Tracking Pixel used both first- and third-party cookies.
3 A first-party cookie is “created by the website the user is visiting”—*i.e.*, Defendant’s
4 Website.⁴⁰ A third-party cookie is “created by a website with a domain name other
5 than the one the user is currently visiting”—*i.e.*, Facebook.⁴¹ The _fbp cookie was
6 always transmitted as a first-party cookie. A duplicate _fbp cookie was sometimes
7 sent as a third-party cookie, depending on whether the browser had recently logged
8 into Facebook.

9 49. Facebook, at a minimum, used the fr, _fbp, and c_user cookies to link to
10 Facebook IDs and corresponding Facebook profiles. Defendant sent these identifiers
11 alongside the event data.

12 50. Plaintiff never consented, agreed, authorized, or otherwise permitted
13 Defendant to disclose his personally identifiable information and protected health
14 information. Plaintiff was never provided with any written notice that Defendant
15 disclosed the protected health information of users of the Website, nor was he
16 provided any means of opting out of such disclosures. Defendant nonetheless
17 knowingly disclosed Plaintiff’s protected health information to Facebook.

18 51. By law, Plaintiff is entitled to privacy in his protected health
19 information and confidential communications. Defendant deprived Plaintiff of his
20 privacy rights when it: (1) implemented a system that surreptitiously tracked,
21 recorded, and disclosed Plaintiff’s and other online patients’ confidential
22 communications, personally identifiable information, and protected health
23 information; (2) disclosed patients’ protected health information to Facebook—an

24 ³⁹ Also confirmable through developer tools.

25 ⁴⁰ PC MAG, FIRST-PARTY COOKIE, [https://www.pcmag.com/encyclopedia/term/first-](https://www.pcmag.com/encyclopedia/term/first-party-cookie)
26 [party-cookie](https://www.pcmag.com/encyclopedia/term/first-party-cookie). This is confirmable by using developer tools to inspect a website’s
cookies and track network activity.

27 ⁴¹ PC MAG, THIRD-PARTY COOKIE, [https://www.pcmag.com/encyclopedia/term/third-](https://www.pcmag.com/encyclopedia/term/third-party-cookie)
28 [party-cookie](https://www.pcmag.com/encyclopedia/term/third-party-cookie). This is also confirmable by tracking network activity.

1 unauthorized third-party eavesdropper; and (3) undertook this pattern of conduct
2 without notifying Plaintiff and without obtaining his express written consent.
3 Plaintiff did not discover that Defendant disclosed his personally identifiable
4 information and protected health information to Facebook, and assisted Facebook
5 with intercepting her communications, until December 2023.

6 **F. Federal Warning on Tracking Codes on Healthcare**
7 **Websites**

8 52. The government has issued guidance warning that tracking code like the
9 Facebook Tracking Pixel may violate federal privacy law when installed on
10 healthcare websites such as Defendant's. The statement titled, USE OF ONLINE
11 TRACKING TECHNOLOGIES BY HIPAA COVERED ENTITIES AND
12 BUSINESS ASSOCIATES (the "Bulletin"), was issued by the Department of Health
13 and Human Services' Office for Civil Rights ("OCR") in December 2022.⁴²

14 53. Healthcare organizations regulated under the Health Insurance
15 Portability and Accountability Act (HIPAA) may use third-party tracking tools, such
16 as the Facebook Tracking Pixel, in a limited way, to perform analysis on data key to
17 operations. They are not permitted, however, to use these tools in a way that may
18 expose patients' PHI to these vendors. The Bulletin explains:

19 Regulated entities [those to which HIPAA applies] are not permitted to use
20 tracking technologies in a manner that would result in impermissible disclosures
21 of PHI to tracking technology vendors or any other violations of the HIPAA
22 Rules. *For example, disclosures of PHI to tracking technology vendors for*
23 *marketing purposes, without individuals' HIPAA-compliant authorizations,*
*would constitute impermissible disclosures.*⁴³

24 54. The bulletin discusses the types of harm that disclosure may cause to the
25 patient:

26 ⁴² HHS.gov, USE OF ONLINE TRACKING TECHNOLOGIES BY HIPAA COVERED
27 ENTITIES AND BUSINESS ASSOCIATES, [https://www.hhs.gov/hipaa/for-](https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html)
28 [professionals/privacy/guidance/hipaa-online-tracking/index.html](https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html).

⁴³ *Id.* (Emphasis added.)

1 An impermissible disclosure of an individual's PHI not only violates the
2 Privacy Rule but also may result in a wide range of additional harms to
3 the individual or others. For example, an impermissible disclosure of PHI
4 may result in identity theft, financial loss, *discrimination, stigma, mental*
5 *anguish, or other serious negative consequences to the reputation,*
6 *health, or physical safety of the individual or to others identified in the*
7 *individual's PHI.* Such disclosures can reveal incredibly sensitive
8 information about an individual, *including diagnoses, frequency of visits*
9 *to a therapist or other health care professionals, and where an*
10 *individual seeks medical treatment.* While it has always been true that
11 regulated entities may not impermissibly disclose PHI to tracking
12 technology vendors, *because of the proliferation of tracking*
13 *technologies collecting sensitive information, now more than ever, it is*
14 *critical for regulated entities to ensure that they disclose PHI only as*
15 *expressly permitted or required by the HIPAA Privacy Rule.*⁴⁴

16 55. Plaintiff and the Class face just the risks about which the government
17 expresses concern. Defendant disclosed the fact that Plaintiff's and Class Members'
18 booked eye exams on Defendant's website, which in turn also discloses the health
19 conditions for which they seek a health care provider; the frequency with which they
20 take steps relating to obtaining eye health care; and where they seek medical
21 treatment. This information is, as described by the OCR in its bulletin, "highly
22 sensitive."

23 56. The Bulletin goes on to make clear how broad the government's view of
24 protected information is. It explains:

25 This information might include an individual's medical record number,
26 home or email address, or dates of appointments, as well as an
27 individual's IP address or geographic location, medical device IDs, *or*
28 *any unique identifying code.*⁴⁵

57. Crucially, that paragraph in the government's Bulletin continues:

*All such [individually identifiable health information ("IIHI")]
collected on a regulated entity's website or mobile app generally is PHI,*

⁴⁴ *Id.* (Emphasis added.)

⁴⁵ *Id.* (Emphasis added.)

1 *even if the individual does not have an existing relationship with the*
2 *regulated entity and even if the IIHI, such as IP address or geographic*
3 *location, does not include specific treatment or billing information like*
4 *dates and types of health care services. This is because, when a*
5 *regulated entity collects the individual's IIHI through its website or*
6 *mobile app, the information connects the individual to the regulated*
7 *entity (i.e., it is indicative that the individual has received or will receive*
8 *health care services or benefits from the covered entity), and thus*
9 *relates to the individual's past, present, or future health or health care*
10 *or payment for care.*⁴⁶

11 58. Then, in July 2022, the Federal Trade Commission ("FTC") and the
12 Department of Health and Human Services ("HHS") issued a joint press release
13 warning regulated entities about the privacy and security risks arising from the use of
14 online tracking technologies:

15 The Federal Trade Commission and the U.S. Department of Health and
16 Human Services' Office for Civil Rights (OCR) are cautioning hospitals
17 and telehealth providers [regulated entities] about the privacy and
18 security risks related to the use of online tracking technologies integrated
19 into their websites or mobile apps that may be impermissibly disclosing
20 consumers' sensitive personal health data to third parties.

21 "When consumers visit a hospital's [regulated entity's] website or seek
22 telehealth services, they should not have to worry that their most private
23 and sensitive health information may be disclosed to advertisers and other
24 unnamed, hidden third parties," said Samuel Levine, Director of the
25 FTC's Bureau of Consumer Protection. "The FTC is again serving notice
26 that companies need to exercise extreme caution when using online
27 tracking technologies and that we will continue doing everything in our
28 powers to protect consumers' health information from potential misuse
and exploitation."

"Although online tracking technologies can be used for beneficial
purposes, patients and others should not have to sacrifice the privacy of
their health information when using a hospital's [regulated entity's]
website," said Melanie Fontes Rainer, OCR Director. "OCR continues

⁴⁶ *Id.* (Emphasis added.)

1 to be concerned about impermissible disclosures of health information to
2 third parties and will use all of its resources to address this issue.”

3 The two agencies sent the joint letter to approximately 130 [regulated
4 entities] hospital systems and telehealth providers to alert them about the
5 risks and concerns about the use of technologies, such as the
6 Meta/Facebook pixel and Google Analytics, that can track a user’s online
7 activities. These tracking technologies gather identifiable information
8 about users, usually without their knowledge and in ways that are hard
9 for users to avoid, as users interact with a website or mobile app.

10 In their letter, both agencies reiterated the risks posed by the unauthorized
11 disclosure of an individual’s personal health information to third parties.
12 For example, the disclosure of such information could reveal sensitive
13 information including health conditions, diagnoses, medications, medical
14 treatments, frequency of visits to health care professionals, and where an
15 individual seeks medical treatment.

16 ... Through its recent enforcement actions against BetterHelp, GoodRx
17 and Premom, as well as recent guidance from the FTC’s Office of
18 Technology, the FTC has put companies on notice that they must
19 monitor the flow of health information to third parties that use tracking
20 technologies integrated into websites and apps. The unauthorized
21 disclosure of such information may violate the FTC Act and could
22 constitute a breach of security under the FTC’s Health Breach
23 Notification Rule ... ⁴⁷

24 Therefore, Defendant’s conduct is directly contrary to clear pronouncements
25 by the FTC and HHS.

26 59. In light of, and in addition to, the government’s own issued guidance
27 above, news sources are also warning that tracking code, like the Facebook Tracking
28 Pixel, poses risks of violating federal privacy law and HIPAA:

⁴⁷ Federal Trade Commission, *FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies*, July 20, 2023, <https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking>.

1 Federal regulators are warning [regulated entities] hospital systems and
2 telehealth providers about the data privacy risks of using third-party tracking
3 technologies.

4 These services, like [Facebook Tracking] Pixel or Google Analytics, could
5 violate the Health Insurance Portability and Accountability Act (HIPAA) or
6 Federal Trade Commission (FTC) data security rules, officials said.

7 The FTC and the U.S. Department of Health and Human Services' Office for
8 Civil Rights (OCR) issued a rare joint release announcing that 130 [regulated
9 entities] hospital systems and telehealth providers received a letter warning
10 them about the data privacy and security risks related to the use of online
11 tracking technologies integrated into their websites or mobile apps ... "The
12 compliance buck still stops with you. Furthermore, your company is legally
13 responsible even if you don't use the data obtained through tracking
14 technologies for marketing purposes."⁴⁸

15 Fierce Healthcare also spoke up in an April 3, 2023 article:

16 Nearly all nonfederal acute care hospitals' [regulated entities'] websites track
17 and transfer data to a third party, potentially fueling the unwanted disclosures
18 of patients' sensitive health information and opening up that [regulated entity]
19 hospital to legal liability, according to a recently published University of
20 Pennsylvania analysis.
21 [https://www.healthaffairs.org/doi/full/10.1377/hlthaff.2022.01205]. The
22 census of more than 3,700 hospital [regulated entity] homepages found at least
23 one third-party data transfer among 98.6% of the websites as well as at least
24 one third-party cookie on 94.3%, researchers wrote in Health Affairs.

25 The hospitals' [regulated entities'] homepages had a median of 16 third-party
26 transfers, more of which were found among medium-sized (100 to 499 beds)
27 hospitals, nonprofit hospitals, urban hospitals, health system-affiliated hospitals
28 and those that weren't serving the largest portion of patients in poverty, they
wrote ... Many of these complaints cite Facebook parent company Meta's Pixel
tracker, which a June 2022 investigation from The Markup
[https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-
medical-information-from-hospital-websites] detected on about a third of large
hospitals' websites. That report found evidence that, in some instances, the

⁴⁸ Heather Landi, *Regulators warn hospitals and telehealth companies about privacy risks of Meta, Google tracking tech*, FIERCE HEALTHCARE, July 21, 2023, <https://www.fiercehealthcare.com/health-tech/regulators-warn-hospitals-and-telehealth-companies-about-privacy-risks-meta-google>

1 sensitive data transferred to third parties met the criteria for a HIPAA
2 violation.⁴⁹

3 Health Affairs also published an article in April 2023, stating:

4 By including third-party tracking code on their websites, hospitals [regulated
5 entities] are facilitating the profiling of their patients by third parties. These
6 practices can lead to dignitary harms, which occur when third parties gain access
7 to sensitive health information that a person would not wish to share. These
8 practices may also lead to increased health-related advertising that targets
9 patients, as well as to legal liability for hospitals [regulated entities].⁵⁰

10 60. This is further evidence that the data that Defendant chose to share is
11 protected Personal Information. The sharing of that information was a violation of
12 Class Members' rights.

13 **CLASS ACTION ALLEGATIONS**

14 61. Class Definition: Pursuant to Federal Rule of Civil Procedure 23(a),
15 (b)(1), (b)(3), and/or (c)(4), Plaintiff brings this action on behalf of himself and other
16 similarly situated individuals (the "Class"), defined as California citizens who,
17 during the class period, had their personally identifiable information or protected
18 health information improperly disclosed to Facebook as a result of using
19 www.lenscrafters.com.

20 62. Plaintiff reserves the right to modify the class definition or add sub-
21 classes as necessary prior to filing a motion for class certification.

22 63. The "Class Period" is the time period beginning on the date established
23 by the Court's determination of any applicable statute of limitations, after

24 ⁴⁹ Dave Muoio, *Almost every hospital's homepage is sending visitors' data to third*
25 *parties, study finds*, FIERCE HEALTHCARE, Apr. 3, 2023,
<https://www.fiercehealthcare.com/providers/almost-every-hospital-homepage-sending-visitors-data-third-parties-study-finds>.

26 ⁵⁰ Ari B. Friedman, et al., *Widespread Third-Party Tracking On Hospital Websites*
27 *Poses Privacy Risks For Patients And Legal Liability For Hospitals*, HEALTH
28 AFFAIRS, Vol. 42, No. 24, April 2023,
<https://www.healthaffairs.org/doi/10.1377/hlthaff.2022.01205>.

1 consideration of any tolling, concealment, and accrual issues, and ending on the date
2 of entry of judgement.

3 64. Excluded from the Class is Defendant; any affiliate, parent, or
4 subsidiary of Defendant; any entity in which Defendant has a controlling interest;
5 any officer, director, or employee of Defendant; any successor or assign of
6 Defendant; anyone employed by counsel in this action; any judge to whom this case
7 is assigned, his/her spouse and immediate family members; and members of the
8 judge's staff.

9 65. Numerosity/Ascertainability. Members of the Class are so numerous
10 that joinder of all members would be unfeasible and not practicable. The exact
11 number of Class Members is unknown to Plaintiff at this time; however, it is
12 estimated that there are at least thousands of individuals in the Class. The identity of
13 such membership is readily ascertainable from Defendant's records and non-party
14 Facebook's records.

15 66. Typicality. Plaintiff's claims are typical of the claims of the Class
16 because Plaintiff used www.lenscrafters.com and had his personally identifiable
17 information and protected health information disclosed to Facebook without his
18 express written authorization or knowledge. Plaintiff's claims are based on the same
19 legal theories as the claims of other Class members.

20 67. Adequacy. Plaintiff is fully prepared to take all necessary steps to
21 represent fairly and adequately the interests of the Class Members. Plaintiff's
22 interests are coincident with, and not antagonistic to, those of the members of the
23 Class. Plaintiff is represented by attorneys with experience in the prosecution of
24 class action litigation, generally, and in the emerging field of digital privacy
25 litigation, specifically. Plaintiff's attorneys are committed to vigorously prosecuting
26 this action on behalf of the members of the Class.

27 68. Common Questions of Law and Fact Predominate/Well Defined
28 Community of Interest. Questions of law and fact common to the members of the

1 Class predominate over questions that may affect only individual members of the
2 Class because Defendant has acted on grounds generally applicable to the Class.
3 Such generally applicable conduct is inherent in Defendant's wrongful conduct.
4 Questions of law and fact common to the Class include:

- 5 a. Whether Defendant intentionally tapped the lines of internet
6 communication between patients and their eye health providers;
- 7 b. Whether Defendant's Website surreptitiously recorded personally
8 identifiable information, protected health information, and related
9 communications and subsequently, or simultaneously, disclosed that
10 information to Facebook;
- 11 c. Whether Facebook was a third-party eavesdropper;
- 12 d. Whether Defendant's disclosures of personally identifiable information,
13 protected health information, and related communications constituted an
14 affirmative act of communication;
- 15 e. Whether Defendant's conduct, which allowed Facebook—an
16 unauthorized person—to view Plaintiff's and Class Members'
17 personally identifiable information and protected health information,
18 resulted in a breach of confidentiality;
- 19 f. Whether Defendant violated Plaintiff's and Class Members' privacy
20 rights by using the Facebook Tracking Pixel to record and communicate
21 online patients' FIDs alongside their confidential medical
22 communications;
- 23 g. Whether Plaintiff and Class Members are entitled to damages under
24 CIPA, the CMIA, or any other relevant statute; and
- 25 h. Whether Defendant's actions violated Plaintiff's and Class Members'
26 privacy rights as provided by the California Constitution.

27 69. Superiority. Class action treatment is a superior method for the fair and
28 efficient adjudication of the controversy. Such treatment will permit a large number

1 of similarly situated persons to prosecute their common claims in a single forum
2 simultaneously, efficiently, and without the unnecessary duplication of evidence,
3 effort, or expense that numerous individual actions would engender. The benefits of
4 proceeding through the class mechanism, including providing injured persons or
5 entities a method for obtaining redress on claims that could not practicably be
6 pursued individually, substantially outweighs potential difficulties in management of
7 this class action. Plaintiff knows of no special difficulty to be encountered in
8 litigating this action that would preclude its maintenance as a class action.

9 **COUNT I**
10 **Violation of the California Invasion of Privacy Act,**
11 **Cal. Penal Code § 631**

12 70. Plaintiff repeats the allegations contained in the paragraphs above as if
13 fully set forth herein and brings this count individually and on behalf of the members
14 of the Class.

15 71. The California Invasion of Privacy Act (“CIPA”) is codified at Cal.
16 Penal Code §§ 630 to 638. CIPA begins with its statement of purpose—namely, that
17 the purpose of CIPA is to “protect the right of privacy of the people of [California]”
18 from the threat posed by “advances in science and technology [that] have led to the
19 development of new devices and techniques for the purpose of eavesdropping upon
20 private communications ... ” Cal. Penal Code § 630.

21 72. A person violates California Penal Code § 631(a), if:

22 by means of any machine, instrument, or contrivance, or in any other
23 manner, [s/he] intentionally taps, or makes any unauthorized
24 connection, whether physically, electrically, acoustically, inductively, or
25 otherwise, with any telegraph or telephone wire, line, cable, or
26 instrument, including the wire, line, cable, or instrument of any internal
27 telephonic communication system, or [s/he] willfully and without the
28 consent of all parties to the communication, or in any unauthorized
manner, reads, or attempts to read, or to learn the contents or meaning
of any message, report, or communication while the same is in transit or
passing over any wire, line, or cable, or is being sent from, or received

1 at any place within this state; or [s/he] uses, or attempts to use, in any
2 manner, or for any purpose, or to communicate in any way, any
3 information so obtained ...

4 Cal. Penal Code § 631(a).

5 73. Further, a person violates § 631(a) if s/he “aids, agrees with, employs,
6 or conspires with any person or persons to unlawfully do, or permit, or cause to be
7 done any of the acts or things mentioned” in the preceding paragraph. *Id.*

8 74. To avoid liability under § 631(a), a defendant must show it had the
9 consent of all parties to a communication.

10 75. At all relevant times, Defendant aided, agreed with, and conspired with
11 Facebook to track and intercept Plaintiff’s and Class Members’ internet
12 communications while accessing www.lenscrafters.com. These communications
13 were intercepted without the authorization and consent of Plaintiff and Class
14 Members.

15 76. Defendant, when aiding and assisting Facebook’s wiretapping, intended
16 to help Facebook learn some meaning of the content in the URLs and the content the
17 visitor requested.

18 77. The following items constitute “machine[s], instrument[s], or
19 contrivance[s]” under the CIPA, and even if they do not, the Facebook Tracking
20 Pixel falls under the broad catch-all category of “any other manner”:

- 21 a. The computer codes and programs Facebook used to track Plaintiff and
22 Class Members’ communications while they were navigating
23 www.lenscrafters.com;
- 24 b. Plaintiff’s and Class Members’ browsers;
- 25 c. Plaintiff’s and Class Members’ computing and mobile devices;
- 26 d. Facebook’s web and ad servers;
- 27 e. The web and ad-servers from which Facebook tracked and intercepted
28 Plaintiff’s and Class Members’ communications while they were using

1 a web browser to access or navigate www.lenscrafters.com;

2 f. The computer codes and programs used by Facebook to effectuate its
3 tracking and interception of Plaintiff's and Class Members'
4 communications while they were using a browser to visit
5 www.lenscrafters.com; and

6 g. The plan Facebook carried out to effectuate its tracking and interception
7 of Plaintiff's and Class Members' communications while they were
8 using a web browser or mobile device to visit www.lenscrafters.com.

9 78. The patient communication information that Defendant transmitted
10 using the Facebook Tracking Pixel, such as eye exam appointment booking
11 information, constituted protected health information.

12 79. As demonstrated hereinabove, Defendant violated CIPA by aiding and
13 permitting third parties to receive its patients' online communications through the
14 Website without their consent.

15 80. As a result of the above violations, Defendant is liable to Plaintiff and
16 other Class Members in the amount of, the greater of, \$5,000 dollars per violation or
17 three times the amount of actual damages. Additionally, Cal. Penal Code § 637.2
18 specifically states that "[it] is not a necessary prerequisite to an action pursuant to
19 this section that the plaintiff has suffered, or be threatened with, actual damages."

20 81. Under the statute, Defendant is also liable for reasonable attorney's fees,
21 and other litigation costs, injunctive and declaratory relief, and punitive damages in
22 an amount to be determined by a jury, but sufficient to prevent the same or similar
23 conduct by Defendant in the future.

24 **COUNT II**

25 **Violation of the California Confidentiality of Medical Information Act Cal. Civ. Code § 56.10**

26 82. Plaintiff repeats the allegations contained in the foregoing paragraphs as
27 if fully set forth herein and brings this claim individually and on behalf of the
28

1 proposed Class.

2 83. Under the California Confidentiality of Medical Information Act, Cal.
3 Civ. Code § 56.10 (“CMIA”), providers of health care are prohibited from disclosing
4 medical information relating to their patients without a patient’s authorization.
5 Medical information refers to “any individually identifiable information, in
6 electronic or physical form, in possession of or derived from a provider of health
7 care ... regarding a patient’s medical history, mental or physical condition, or
8 treatment. “Individually Identifiable” means that the medical information includes
9 or contains any element of personal identifying information sufficient to allow
10 identification of the individual ... ”

11 84. Plaintiff and Class Members are patients under the definition of the
12 CMIA because Plaintiff and Class Members received “health care services from a
13 provider of health care” and the information Defendant shared to Facebook was
14 “medical information pertain[ing]” to Plaintiff and Class Members. Cal. Civ. Code §
15 56.05(m).

16 85. Defendant is a “provider of health care” as defined in Cal. Civ. Code §
17 56.05(p) because Defendant offers optometry services. Defendant is also considered
18 a “provider of health care” under Cal. Civ. Code § 56.06, subdivisions (a) and (b),
19 because Defendant’s Website maintains medical information and offers software to
20 consumers that is designed to maintain medical information for the purposes of
21 allowing its users to manage their information or make the information available to a
22 health care provider, of for the diagnoses, treatment, or management of a medical
23 condition.

24 86. Therefore, as a provider of health care, Defendant is subject to the
25 requirements of the CMIA and had an ongoing obligation to comply with the
26 CMIA’s requirements regarding the maintenance of its user’s medical information.

27 87. As set forth hereinabove, a Facebook ID is an identifier sufficient to
28 allow identification of an individual. Along with patients’ Facebook ID, Defendant

1 disclosed to Facebook several pieces of information regarding its patients' use of
2 Defendant's Website, which, on information and belief, included, but was not limited
3 to: patient medical conditions and treatment patients were seeking such as scheduling
4 eye exam appointments searched for by patients.

5 88. This patient information was derived from a provider of health care
6 regarding patients' medical treatment and physical condition. Accordingly, it
7 constituted medical information pursuant to the CMIA.

8 89. As demonstrated hereinabove, Defendant failed to obtain its patients'
9 valid authorization for the disclosure of medical information.

10 90. Pursuant to CMIA § 56.11, a valid authorization for disclosure of
11 medical information must: (1) be "[c]learly separate from any other language present
12 on the same page and is executed by a signature which serves no other purpose than
13 to execute the authorization"; (2) be signed and dated by the patient or her
14 representative; (3) state the name and function of the third party that receives the
15 information; and (4) state a specific date after which the authorization expires.
16 Accordingly, information set forth in Defendant's Website Privacy Policy does not
17 qualify as a valid authorization.

18 91. Based on the above, Defendant violated the CMIA by disclosing its
19 patients' medical information with Facebook along with the patients' Facebook IDs.

20 92. Under the CMIA, a patient may recover compensatory damages,
21 punitive damages not to exceed \$3,000 dollars and attorneys' fees not to exceed
22 \$1,000, and the costs of litigation for any violating disclosure of medical
23 information. Alternatively, a patient may recover nominal damages of \$1,000 for
24 any negligent release of medical information.

25 **COUNT III**

26 **Invasion of Privacy Under California's Constitution**

27 93. Plaintiff repeats the allegations contained in the foregoing paragraphs as
28 if fully set forth herein and brings this claim individually and on behalf of the

1 proposed Class.

2 94. Plaintiff and Class Members have an interest in: (1) precluding the
3 dissemination and/or misuse of their sensitive, confidential communications and
4 protected health information; and (2) making personal decisions and/or conducting
5 personal activities without observation, intrusion or interference, including, but not
6 limited to, the right to visit and interact with various internet sites without being
7 subjected to wiretaps without Plaintiff's and Class Members' knowledge or consent.

8 95. At all relevant times, by using the Facebook Tracking Pixel to record
9 and communicate patients' Facebook IDs alongside their confidential medical
10 communications, Defendant intentionally invaded Plaintiff's and Class Members'
11 privacy rights under the California Constitution.

12 96. Plaintiff and Class Members had a reasonable expectation that their
13 communications, identities, health information, and other data would remain
14 confidential and that Defendant would not install wiretaps on www.lenscrafters.com.

15 97. Plaintiff and Class Members did not authorize Defendant to record and
16 transmit Plaintiff's and Class Members' private medical communications alongside
17 their personally identifiable health information.

18 98. This invasion of privacy was serious in nature, scope, and impact
19 because it related to patients' private medical communications. Moreover, it
20 constituted an egregious breach of the societal norms underlying the privacy right.

21 99. Accordingly, Plaintiff and Class Members seek all relief available for
22 invasion of privacy claims under California's Constitution.

23 **PRAYER FOR RELIEF**

24 WHEREFORE, Plaintiff prays for relief and judgment, as follows:

- 25 a. For a determination that this action is a proper class action;
26 b. For an order certifying the Class, naming Plaintiff as
27 representative of the Class, and naming Plaintiff's attorneys as
28 Class Counsel to represent the Class;

- c. For an order declaring that Defendant's conduct violated the statutes referenced herein;
- d. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;
- e. For an award of compensatory damages, including statutory damages where available, to Plaintiff and the Class Members against Defendant for all damages sustained as a result of Defendant's wrongdoing, in an amount to be proven at trial;
- f. For punitive damages, as warranted, in an amount to be determined at trial;
- g. For an order requiring Defendant to disgorge revenues and profits wrongfully obtained;
- h. For prejudgment interest on all amounts awarded;
- i. For injunctive relief as pleaded or as the Court may deem proper;
- j. For an order awarding Plaintiff and the Class their reasonable attorneys' fees and expenses and costs of suit; and
- k. For an order granting Plaintiff and Class members such further relief as the Court deems appropriate.

DEMAND FOR JURY TRIAL

Plaintiff on behalf of himself and the proposed Class, demands a trial by jury for all of the claims asserted in this Complaint so triable.

Dated: January 23, 2024

Respectfully submitted,

BURSOR & FISHER, P.A.

By: /s/ L. Timothy Fisher
L. Timothy Fisher

L. Timothy Fisher (State Bar No. 191626)
Brittany S. Scott (State Bar No. 327132)

1 1990 North California Blvd., Suite 940
2 Walnut Creek, CA 94596
3 Telephone: (925) 300-4455
4 Facsimile: (925) 407-2700
5 E-mail: ltfisher@bursor.com
6 bscott@bursor.com

7 *Attorneys for Plaintiff and the Putative Class*
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28